

REMARKS

Reconsideration and withdrawal of the rejections set forth in the Office Action dated October 20, 2004, are respectfully requested. A separate petition for a two-month extension of time accompanies this amendment.

The applicant's representative wishes to thank Examiners Tran and Morse for the interview on February 1, 2005. During the interview, the parties discussed background technology, prior art (including U.S. Patent No. 5,682,430 to Killian et al.), applicant's system, and claims 1, 6, 10, 18, 28 and 35. The applicant discussed that the prior art did not show proof of correctness for a shuffled sequence of electronic data elements based on a scaled iterated logarithmic multiplication proof. Further details regarding the substance of the interview may be found below. If Examiners Tran or Morse believe that any additional information regarding the interview is necessary, please let the undersigned attorney know.

The Office Action indicated that the drawings are both acceptable and objected to by the Examiner. During the interview, it was agreed that the drawings were acceptable. However, if that is incorrect, please let the undersigned attorney know.

During the interview, the applicant's representative noted that information disclosure statements provided on July 12, 2001 and June 25, 2003 had not been initialed and returned. Examiner Tran indicated that she would ensure that the information disclosure statements were received, initialed, and a copy returned. If, however, these information disclosure statements cannot be found, the applicant's representative can provide replacement copies.

I. Amendments

Claim 18 is being amended to note that the cryptographic relationship employed under the invention of claim 18 uses scaled iterated logarithmic multiplication. Support for this limitation may be found, for example, in other, previously pending claims, such as claims 1, 6, 10, 28 and 35.

Additionally, the term "linear size" has been deleted from claims 1, 6, 10, 28 and 35.

IV. Rejections under 35 U.S.C. § 102

A. The Applied Art

Claims 6, 9-18, 26, 27, 28, and 30-35 are rejected under 35 U.S.C. § 102(e) as being anticipated by Challener et al. (U.S. Patent No. 6,081,793, hereinafter Challener).¹ While Challener discloses a cryptographic system for electronic voting, it lacks aspects of the claimed invention, including a system employing "scaled iterated logarithmic multiplication," as discussed below.

B. Analysis

The shuffling or mixing of ballots is known, such as is described in Killian et al. However, the system of Killian is impractical because it requires far too many computations to be commercially practical with a large number of ballots to shuffle.

The claimed invention employs "scaled iterated logarithmic multiplication" that generates proofs of correctness in the shuffling/mixing of ballot/data elements to prove that the input elements/ballots are equivalent to the output ballots/elements, except for the shuffling. Iterated logarithmic multiplication provides a novel technique to improve shuffling over prior systems, and is described in detail on pages 10-12 of the application. While the Killian reference does disclose a shuffle-based cryptographic technique, the presently claimed invention improves significantly over this technique, because the size and number of computations needed is orders of magnitude less than that of Killian.

During the interview, concern was raised regarding the term "linear size" as being possibly vague. Applicant disagrees: the term "linear size" is believed to be clear from both the wording of the claims and the detailed description provided in the application. Further, one skilled in the art is believed to unambiguously and readily understand that the term "linear size" refers to a complexity of the described embodiments, and particularly to a number of arithmetic operations to be performed. In this sense, it is believed that those of ordinary skill will readily understand that "linear

¹ Silence regarding the position taken, or argument made, by the Examiner does not indicate any acquiescence to that position or argument. Furthermore, arguments made with respect to a particular claim or claims apply only to that claim or claims, and not to other claims, unless specifically noted herein.

size" means linear with the number of encrypted data elements to be shuffled. Nevertheless, to overcome such a possible objection, the term "linear size" has been deleted from the claims. Deleting this expression is believed to overcome any objection on the one hand, and on the other does not improperly expand the scope of the claimed subject matter. In other words, the claims are patentable despite such language, in part because of the use of "scaled iterated logarithmic multiplication" in the claimed cryptographic operations.²

V. Rejections under 35 U.S.C. § 103

A. The Applied Art

Claims 1-4, 7, 8, 19-25, and 29 are rejected under 35 U.S.C. § 103(a) as being unpatentable over '793 further in view of Kilian et al. (U.S. Patent No. 5,682,430, hereinafter '430).

Claim 5 is rejected under 35 U.S.C. § 103(a) as being unpatentable over '793 further in view of '430 and further in view of Davis et al. (U.S. Patent No. 6,550,675, hereafter '675).

B. Analysis

Claim 1 recites, among other limitations, "scaled iterated logarithmic multiplication." For at least this reason, claim 1 is patentable, as noted above. Further, claims 2-5, 7, 8, 19-25 and 29 are dependent claims, and are thus patentable for the reasons noted above for their corresponding independent claims.

VI. Conclusion

Overall, none of the applied references, singly or in any motivated combination, teach or suggest the features recited in independent claims 1, 6, 10, 18, 28 and 35, and thus such claims are allowable. Since these independent claims are allowable, based at least on the above reasons, the claims which depend from them are likewise

² Claims substantially similar to those currently pending are about to issue in both Europe and Canada (i.e., claims which recite "scaled iterated logarithmic multiplication", but which omit "linear size"). While proof of this was provided during the interview, if the Examiner would like any additional evidence of this, please let the undersigned attorney know.

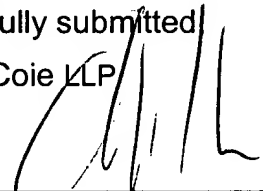
allowable. If the undersigned attorney has overlooked a relevant teaching in any of the references, the Examiner is requested to point out specifically where such teaching may be found.

In view of the foregoing, the claims pending in the application comply with the requirements of 35 U.S.C. § 112 and patentably define over the applied art. A Notice of Allowance is, therefore, respectfully requested. If the Examiner has any questions or believes a telephone conference would expedite prosecution of this application, the Examiner is encouraged to call the undersigned at (206) 359-3599.

Date: _____

3/21/05

Respectfully submitted
Perkins Coie LLP



Christopher J. Daley-Watson
Registration No. 34,807

Correspondence Address:

Customer No. 25096
Perkins Coie LLP
P.O. Box 1247
Seattle, Washington 98111-1247
(206) 359-8000